Secure Systems Design and Technology Development. Veliko Tarnovo, Bulgaria
Proceedings of the International Scientific Conference, 2026. Volume I, 321-327

A Hybrid Probabilistic and FMEA-Based Model for Reliability and Fault Tolerance Assessment of AI-Based Security Systems

Silvia Nikolova
Faculty of Technical Sciences
Konstantin Preslavsky University of Shumen
Shumen, Bulgaria
silvia_nikolova73@abv.bg

Tsvetoslav Tsankov
Faculty of Technical Sciences
Konstantin Preslavsky University of Shumen
Shumen, Bulgaria
c.cankov@shu.bg

Abstract. **This study presents a hybrid approach that integrates probabilistic modeling and Failure Mode and Effects Analysis (FMEA) for the analysis and optimization of reliability and fault tolerance in AI-driven integrated security systems. With the increasing complexity of modern intelligent systems—incorporating video analytics, Internet of Digital Things (IoDT) sensors, autonomous drones, and distributed computing infrastructures—there is a growing need for comprehensive methods to evaluate system risk and resilience. A mathematical model based on stochastic processes and Markov chains is developed, enabling quantitative evaluation of failure probabilities and transitions between key system states, including normal operation, degraded mode, and complete failure. In parallel, an FMEA analysis is applied to identify critical components, assess the consequences of potential failures, and calculate Risk Priority Numbers (RPN). The proposed hybrid model integrates probabilistic assessments with expert-driven engineering analysis, resulting in improved accuracy in reliability evaluation. A system-level analysis is conducted across the main subsystems, including the sensing layer, AI processing modules, communication infrastructure, and robotic response units. The results indicate that the communication network and AI modules represent the most critical elements in terms of failure risk. The proposed methodology can be applied in the design, optimization, and management of intelligent security systems, contributing to enhanced robustness, reliability, and operational efficiency under real-world conditions.**

Keywords: Artificial intelligence, Fault tolerance, FMEA analysis, Intelligent security systems.

I. INTRODUCTION

A. Relevance of the problem

Modern security systems are undergoing a significant transformation driven by the development of artificial intelligence (AI), the Internet of Things (IoT/IoDT) and autonomous robotic platforms. Integrated security systems now include multiple interconnected components – video surveillance with intelligent analytics, distributed sensor networks, unmanned aerial vehicles and cloud infrastructures [1]–[4].

This complexity leads to increased requirements for the reliability, availability and fault tolerance of systems, especially when protecting critical infrastructure, industrial sites and urban environments. Failure of an individual component can lead to a significant reduction in efficiency or to a complete failure of the system [5]–[7].

B. Scientific problem

Traditional reliability analysis methods based on classical probabilistic models are often not sufficient for the assessment of complex intelligent systems. On the other hand, methods such as FMEA provide qualitative and expert assessment, but do not include the dynamic behavior of the system over time [8]–[11].

An integrated approach that combines quantitative probabilistic assessment, engineering expert risk assessment and dynamic system behavior is lacking.

This problem is central to modern reliability theory for critical infrastructures, autonomous systems and IoT. Traditional methods (FTA, RBD) often suffer from a lack of failure data for new technologies, while FMEA is a "static snapshot" of risk, not a description of the process over time.

Existing reliability assessment methods such as Fault Tree Analysis (FTA), Reliability Block Diagrams (RBD), and classical probabilistic approaches provide effective mathematical evaluation of hardware reliability but often fail to represent adaptive AI behavior and algorithmic uncertainty. At the same time, traditional FMEA approaches support engineering risk assessment but remain

Online ISSN 3044-7771
https://doi.org/10.68302/std2026.vol1.136

predominantly static and qualitative. Modern intelligent security systems introduce additional challenges related to false classifications, model drift, adversarial inputs, distributed decision-making, and communication dependency, which are insufficiently addressed in conventional reliability methodologies [12]–[15].

The proposed hybrid approach attempts to bridge this gap by integrating probabilistic state modeling with expert-oriented FMEA analysis, enabling simultaneous evaluation of stochastic system dynamics and engineering risk prioritization.

In order to integrate quantitative probabilistic assessment, engineering expert assessment (qualitative risk) and dynamic behavior, it is necessary to combine several methods in a hybrid framework.

C. *Purpose of the study: Failure Modes and Effects Analysis (FMEA)*

The main objective of this study is to develop a hybrid model that combines Probabilistic Modeling and Failure Modes and Effects Analysis (FMEA) for reliability assessment, fault tolerance analysis, and architecture optimization of intelligent security systems. This hybrid approach overcomes the limitations of traditional qualitative FMEA by introducing quantitative risk assessment.

D. *Research objectives*

To achieve the goal, the following tasks are formulated:

- Development of a mathematical probabilistic model
- Modeling of states through Markov processes
- Conducting an FMEA analysis
- Identification of critical components
- Integration of different approaches
- Analysis and optimization of the system

E. *Scientific contribution*

This research contributes to the field of reliability of intelligent systems by developing an integrated hybrid model combining probabilistic analysis and FMEA. This is achieved by adapting classical methods to AI-based systems and introducing an algorithmic risk assessment approach. The result is the identification of critical components in integrated security systems and the creation of a methodology for optimizing the fault tolerance of intelligent systems [16]–[18].

II. MATERIALS AND METHODS

A. *Architecture of the studied system*

The considered intelligent security system TEDI (Technological, Electronic, Digital Intelligence) represents an integrated multi-layered structure that includes a variety of interconnected elements (Fig. 1):

- Sensor layer – video cameras, IoDT, sensors (motion, temperature, vibration)
- Processing layer – Edge AI (local processing), Cloud AI (centralized processing)

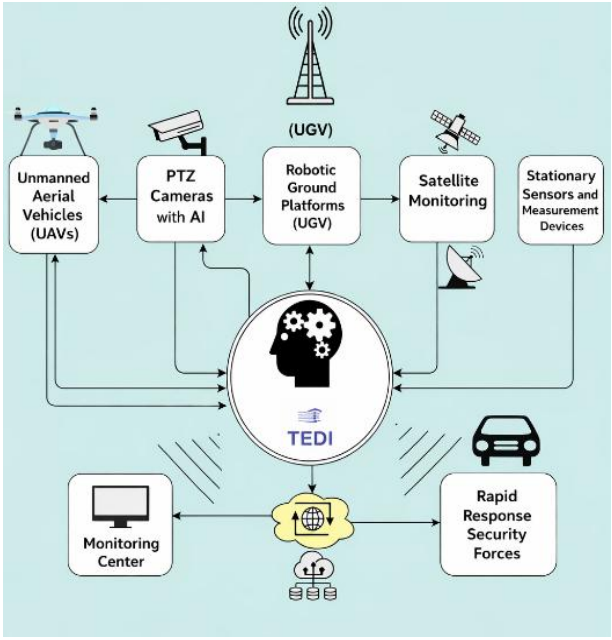

Fig. 1. Architecture of TEDI.

- Communication infrastructure – optical network, wireless communication (5G/LTE), backup channels
- Response layer – autonomous drones, robotic systems, alarm mechanisms

The considered intelligent security system is modeled as a complex stochastic system composed of multiple interconnected subsystems:

$$S = \{S1, S2, \ldots, Sn\} \quad (1)$$

where each subsystem Si is characterized by:

- failure rate λ_i
- recovery rate μ_i
- reliability function $R_i(t)$

The system is considered as a combined serial-parallel structure, reflecting the real architecture of intelligent systems [19]–[21].

B. *Probabilistic reliability model*

Time-to-failure modeling

The time to failure of components is assumed to follow an exponential distribution:

$$R_i(t) = e^{-\lambda_i t} \quad (2)$$

where:

λ_i – failure intensity

System reliability

For a combined structure:

$$R_{\text{system}} = R_{\text{sensor}} * R_{\text{AI}} * R_{\text{comm}} * R_{\text{response}} \quad (3)$$

Parallel structure:

$$R = 1 - (1 - R_1)(1 - R_2) \quad (4)$$

Sequential structure:

$$R = \prod R_i \quad (5)$$

Markov model

The system is modeled using three states:

- S_0 – normal state
- S_1 – degraded state
- S_2 – complete failure

The degraded state S_1 represents partial operational capability caused by subsystem degradation, including communication instability, reduced AI inference accuracy, sensor malfunction, or temporary drone unavailability. The failed state S_2 corresponds to critical operational interruption resulting from simultaneous subsystem failures or unsuccessful recovery processes. Transition probabilities between the states are influenced by redundancy mechanisms, backup communication channels, and recovery procedures integrated within the intelligent security architecture.

Transition matrix:

$$Q = \begin{pmatrix} -\lambda & \lambda & 0 \\ \mu & -(\lambda_r + \mu) & \lambda_r \\ 0 & 0 & 0 \end{pmatrix} \quad (6)$$

The probabilistic behavior is described by:

$$\frac{dP(t)}{dt} = P(t)Q \quad (7)$$

Where:
λ – failure rate
λ_r – backup failure rate
μ – recovery rate

The recovery transition μ reflects the ability of the system to restore operational functionality through redundancy, fault-tolerant architecture, and automated recovery mechanisms.

C. FMEA analysis

Failure Identification

The following subsystems were analyzed:

- cameras
- AI modules
- communication
- drones
- database

Risk Assessment

Each failure is assessed by:

- Severity (S)
- Occurrence (O)
- Detection (D)

Risk index calculation RPN

$$RPN = S \cdot O \cdot D \quad (8)$$

D. Integrated hybrid model

The proposed model combines a probabilistic and FMEA approach:

$$P_{failure} \leftrightarrow RPN \quad (9)$$

Through:

$$Risk_{total} = \alpha P_{\text{failure}} + \beta \frac{RPN}{RPN_{max}} \quad (10)$$

where:

RPN – The traditional risk priority number

$Risk_{total}$ – The final, summarized risk assessment for a specific failure mode.

α – Weighting factor for the probability of failure.

β – Weighting factor for the RPN result.

α, β ∈ [0,1], α + β = 1

$P_{failure}$ – Probability of failure occurrence.

RPN_{max} – The maximum possible value of RPN.

In the present study, the weighting coefficients are selected as α = 0.6 and β = 0.4 in order to provide a stronger influence of probabilistic reliability assessment while preserving the engineering significance of the FMEA evaluation. The selected balance allows simultaneous consideration of stochastic system behavior and expert-based risk prioritization. Higher α values increase the influence of probabilistic failure behavior, while higher β values emphasize engineering risk evaluation through the RPN methodology.

E. Summary of the methodology

The proposed methodology can be reproduced using the presented probabilistic equations, Markov transition structure, and FMEA evaluation procedure. The numerical experiment represents a demonstrative engineering scenario intended to illustrate the applicability of the hybrid model in intelligent security architectures. The sequence of analysis includes subsystem reliability estimation, stochastic state transition modeling, FMEA-based risk evaluation, normalization of results, and integrated hybrid risk assessment.

III. Results and Discussion

A. Numerical experiment setup

To evaluate the proposed model, an integrated security system with the following subsystems is considered (Table 1):

TABLE 1 SUBSYSTEM RELIABILITY PARAMETERS

Subsystem	Label	Failure Rate λ [1/h]	Repair Rate μ [1/h]
Cameras	S_1	0.002	0.05
IoDT Sensors	S_2	0.0015	0.04
AI Module	S_3	0.003	0.06
Communication Network	S_4	0.004	0.05
Drones	S_5	0.0025	0.045

Calculation of the reliability of individual components for t=100 hours:

$$R_i(t) = e^{-\lambda_i t} \quad (11)$$

Calculation of the reliability of cameras:

$$R_1 = e^{-0.002.100} = e^{-0.002} \approx 0.8187 \quad (12)$$

The failure and repair rates used in the numerical experiment are based on representative values from reliability engineering literature, intelligent surveillance systems, industrial communication infrastructures, and expert engineering assumptions. Due to the limited availability of publicly accessible operational datasets for integrated AI-based security systems, several parameters are selected as illustrative values intended to demonstrate the applicability and behavior of the proposed hybrid reliability model.

The communication subsystem is assigned a relatively higher failure rate due to its critical role in distributed data exchange and dependency on network availability. The AI module incorporates both hardware-related and algorithmic reliability factors, while the drone subsystem reflects combined navigation, battery, and communication risks [22]–[24].

$$R_2 = e^{-0.15} \approx 0.8607 \quad (13)$$

Calculation of the reliability of AI:

$$R_3 = e^{-0.03} \approx 0.7408 \quad (14)$$

Calculation of communication reliability:

$$R_4 = e^{-0.04} \approx 0.6703 \quad (15)$$

Calculation of drone reliability:

$$R_5 = e^{-0.25} \approx 0.7788 \quad (16)$$

As a result, the overall reliability of the system with a sequential structure is:

$$R_{system} = R_1 \cdot R_2 \cdot R_3 \cdot R_4 \cdot R_5 \quad (17)$$

$$R_{system} \approx 0.8187 \cdot 0.8607 \cdot 0.7408 \cdot 0.6703 \cdot 0.7788 \approx 0.272 \quad (18)$$

with probability of failure:

$$P_{failure} = 1 - 0.272 = 0.728 \quad (19)$$

The overall reliability with parallel redundancy of the communication with these results is:

$$R_{comm} = 1 - (1 - R_4)^2 \quad (20)$$

$$R_{comm} = 1 - (1 - 0.67)^2 = 1 - (0.32)^2 \approx 0.891 \quad (21)$$

From which a new system reliability is obtained:

$$R_{system,new} = R_1 \cdot R_2 \cdot R_3 \cdot R_{comm} \cdot R_5 \quad (22)$$

$$R_{system,new} \approx 0.8187 \cdot 0.8607 \cdot 0.7408 \cdot 0.8913 \cdot 0.7788 \approx 0.361 \quad (23)$$

The improvement of the system can be calculated by the formula:

$$\Delta R = 0.361 - 0.272 = 0.089 \quad (24)$$

This results in a ≈33% relative improvement in system reliability.

For the Markov numerical analysis, the following values are used:

λ = 0.003
λr = 0.002
μ = 0.05

thus, the probability of failure is calculated as follows:

$$\pi_2 = \frac{\lambda\lambda r}{\mu\lambda r + \mu\lambda + \lambda\lambda r} \approx 0.0234 \quad (25)$$

The probability of complete failure ≈ 2.34% in the presence of recovery, which is a significant improvement over the static model.

FMEA numerical analysis (Table 2)

Normalization of results

$$RPN_{max} = 180 \quad (26)$$

$$RPN_{norm}^{AI} = \frac{162}{180} = 0.9 \quad (27)$$

Risk calculation in a hybrid model – Integrated risk in α = 0.6, β = 0.4*:*

$$Risk = 0.6 \cdot 0.728 + 0.4 \cdot 0.9 = 0.7968 \quad (28)$$

After optimization

TABLE 2 FMEA ANALYSIS OF THE SYSTEM

No.	Subsystem	Failure Mode	Cause	Effect	S	O	D	RPN	Recommended Action
1	Cameras	Video signal loss	Hardware failure	Loss of monitoring	8	4	3	96	Redundant cameras
2	Cameras	Dirty lens	Environmental conditions	Reduced image quality	5	6	5	150	Auto-cleaning system
3	IoDT Sensors	Invalid data	Calibration error	False alarms	6	4	6	144	Periodic calibration
4	AI Analysis	Misclassification	Poor training	Missed incident	9	3	6	162	Model retraining
5	AI Analysis	False positive detection	Model overfitting	Unnecessary alarm activation	6	4	5	120	Model optimization
6	AI Analysis	False negative detection	Poor training dataset	Missed security incident	9	3	6	162	Dataset retraining
7	AI Analysis	Model drift	Environmental changes	Reduced detection accuracy	8	4	5	160	Continuous learning
8	AI Analysis	Adversarial input	Manipulated visual data	Incorrect classification	9	2	7	126	Adversarial defense mechanisms
9	AI Server	GPU failure	Hardware fault	Processing interruption	8	3	4	96	Backup server
10	Communication Network	Connection loss	Network failure	Data interruption	9	4	5	180	Redundant channels
11	Drone 1	GPS loss	Electromagnetic interference	Navigation failure	7	3	5	105	Inertial navigation
12	Drone 2	Battery depletion	Poor management	Mission interruption	6	5	4	120	Battery monitoring
13	Control Center	Server crash	Software issue	Loss of control	9	2	3	54	Cluster architecture
14	Database	Data loss	Disk failure	Loss of records	8	3	4	96	RAID & backup

$$P_{failure,new} = 1 - 0.361 = 0.639 \quad (29)$$

$$Risk_{new} = 0.6 \cdot 0.639 + 0.4 \cdot 0.6 = 0.6234 \quad (30)$$

Final result (Table 3)

B. Main conclusions from the numerical analysis

Probabilistic model results

The developed probabilistic model allows for a quantitative assessment of the system's reliability over time. When applying an exponential distribution to the individual components, it is found that the overall reliability of the system decreases exponentially, with the rate of degradation depending on the total failure intensity.

For the integrated system we obtain:

$$R_i(t) = e^{-\lambda_{eq} t} \quad (31)$$

where:

$$\lambda_{eq} = \sum \lambda_i \quad (32)$$

TABLE 3 SYSTEM PERFORMANCE BEFORE AND AFTER OPTIMIZATION

Metric	Before	After
Reliability	0.272	0.361
Failure Probability	0.728	0.639
Total Risk	0.797	0.623

The analysis shows that:

- without redundancy, the system is highly sensitive to a single component failure
- with parallel redundancy, a significant increase in reliability is observed
- implementing Edge AI reduces dependence on the central server

Results of the Markov model

The solution of the Markov model shows the probability distribution of the states:

- $P_0(t)$ – normal operation
- $P_1(t)$ – degraded state
- $P_2(t)$ – failure

In steady-state mode, it is found that the probability of a degraded mode is significantly higher than that of a complete failure. Increasing the recovery intensity μ leads to a significant decrease in P_2, and redundancy reduces the frequency of transition to a failure state.

Results of the FMEA analysis

The FMEA analysis conducted identifies the critical components of the system through the values of the RPN index.

Highest values: Communication network – RPN = 180

Average values: IoDT sensors – 144

Low values: Control center –54

Graphical analysis of the hybrid model (Fig. 2)

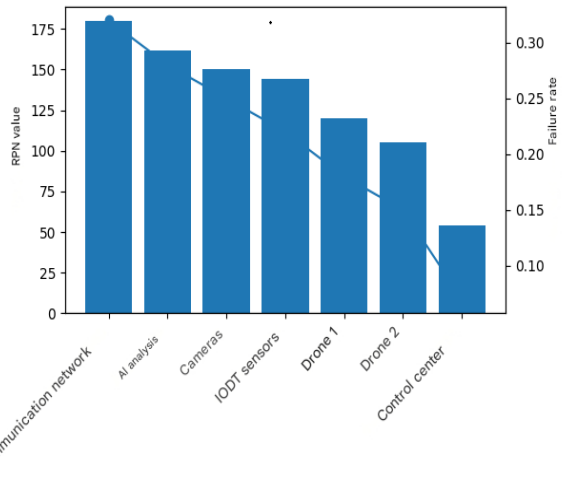

Fig. 2. Risk Priority Number (RPN) Distribution Across System Components.

The graph of RPN values clearly differentiates the criticality of individual components in the system. The highest value is recorded for the communication network (RPN = 180), which defines it as the main source of system risk and a priority for optimization. Components based on artificial intelligence and video surveillance – AI analysis (162) and cameras (150) – also fall into the high-risk zone. This shows that algorithmic errors and the quality of visual data have a significant impact on reliability. IoDT sensors (144) and drones (120–105) form a group with medium-high risk, which suggests the need for additional stabilization, but do not represent a critical failure factor. The control center (54) demonstrates the lowest risk, which positions it as the most resilient component in the architecture.

The results obtained show that the reliability of intelligent security systems is highly dependent on the communication infrastructure, the algorithmic stability of AI and the quality of input data. It is particularly important that AI systems add a new type of risk – algorithmic risk, which does not exist in classical systems.

C. Advantages of the proposed model

The hybrid approach offers an integration of quantitative and qualitative methods for a more accurate risk assessment. This allows for prioritization of engineering solutions and is a prerequisite for applicability to complex distributed systems. Despite the undeniable advantages, the model has a number of limitations of the study. These are the use of an exponential distribution (simplification), dependence on expert assessments in FMEA and limited empirical validation. Future validation using real operational datasets and large-scale deployment scenarios may further improve the precision and applicability of the proposed model.

The proposed model can be used in the design of video surveillance systems for the protection of critical infrastructure. The proposed model can also be applied in the design of Smart City infrastructures and industrial IoT systems.

IV. Conclusions

This study presents a hybrid approach for the analysis and optimization of the reliability of intelligent security systems, based on a combination of probabilistic modeling and FMEA analysis. The results show that the reliability of the system critically depends on the communication infrastructure, with AI modules being a key factor for fault tolerance. The application of the hybrid approach allows for a more accurate risk assessment.

The proposed model provides an effective tool for the analysis of complex systems and the identification of critical components. The evaluation of the results can be a foundation for architecture optimization.

Future research may include Monte Carlo simulations, as they are a powerful mathematical method for modeling uncertainty and predicting outcomes in complex systems. Also, the analysis can be improved using real operational data. A very important factor for predictive maintenance is machine learning and its extension to cybersecurity and hybrid attacks.

The hybrid probabilistic and FMEA approach represents an effective methodology for analyzing the reliability of modern intelligent security systems, providing a balance between mathematical rigor and engineering applicability [25]-[26].

V. Acknowledgement

The authors would like to express their sincere gratitude to their colleagues from the Faculty of Technical Sciences at Konstantin Preslavsky University of Shumen for their valuable support, professional advice, scientific discussions, motivation, and cooperation during the preparation of this research. Their recommendations and constructive feedback contributed significantly to the development and improvement of the present study. This publication is funded by the fund "Support for Publishing Publications in Journals with Impact Factor (IF) and Impact Rank (SJR)" of Konstantin Preslavsky University of Shumen, Republic of Bulgaria.

References

[1] R. Kumar, J. Singh, and Y. K. Dwivedi, "Application of IoT and AI in smart surveillance systems: A systematic review," *Sustainable Cities and Society*, vol. 70, 102889, 2021.

[2] X. Xu et al., "Edge–cloud collaborative intelligence for IoT systems," *Future Generation Computer Systems*, vol. 128, pp. 1–12, 2022.

[3] C. Alcaraz and J. Lopez, "Cybersecurity in IoT-based smart systems: A review," *Computer Networks*, vol. 185, 107731, 2021.

[4] V. Stoyanova, "Analysis of the public communication channels for transmission of hidden information," in *Proc. Int. Conf. Advanced Research and Technology for Defence (ARTDef)*, 2021, ISSN 2815-2581.

[5] Z. Chen, K. Zhang, and H. Li, "Reliability modeling of distributed AI systems in edge-cloud environments," *IEEE Internet of Things Journal*, vol. 9, no. 8, pp. 5678–5690, 2022.

[6] S. Park and J. Kim, "Fault-tolerant architecture for AI-based surveillance systems using edge computing," *Future Generation Computer Systems*, vol. 144, pp. 12–25, 2023.

[7] P. Singh and V. Sharma, "Fault tolerance in distributed IoT systems: A survey," *Computer Communications*, vol. 182, pp. 1–15, 2022.

[8] Y. Zhang, M. Xie, and P. Wang, "Reliability analysis of complex systems using Bayesian networks and AI techniques," *Reliability Engineering & System Safety*, vol. 210, 107530, 2021.

[9] X. Li, H. Chen, and L. Xu, "A hybrid reliability assessment method combining FMEA and Bayesian networks for intelligent systems," *IEEE Access*, vol. 10, pp. 34567–34580, 2022.

[10] Y. Liu and X. Zhao, "Hybrid probabilistic models for reliability optimization in smart systems," *IEEE Systems Journal*, vol. 17, no. 2, pp. 3456–3467, 2023.

[11] Q. Zhou et al., "Integrated FMEA and probabilistic risk analysis for intelligent systems," *Reliability Engineering & System Safety*, vol. 232, 109054, 2023.

[12] Z. Wang and X. Chen, "Hybrid FMEA and Bayesian network for reliability assessment," *Safety Science*, vol. 139, 105239, 2021.

[13] A. Gupta and S. Srivastava, "Failure mode and effect analysis in cyber-physical systems: A review," *Microprocessors and Microsystems*, vol. 90, 104450, 2022.

[14] H. Liu et al., "A novel fuzzy FMEA approach for risk assessment in complex systems," *Applied Soft Computing*, vol. 86, 105899, 2020.

[15] F. Alqahtani and A. Kumar, "Risk assessment of IoT-based smart systems using FMEA and machine learning," *Sensors*, vol. 23, no. 4, 2156, 2023.

[16] T. Wang, Y. Zhao, and L. Sun, "A Markov-based reliability evaluation method for intelligent monitoring systems," *Applied Mathematical Modelling*, vol. 89, pp. 1102–1115, 2021.

[17] B. Sun et al., "Reliability analysis of AI-enabled cyber–physical systems," *IEEE Systems Journal*, vol. 16, no. 4, pp. 5890–5901, 2022.

[18] L. Zhang, X. Wu, and Y. Zhao, "Deep learning-based reliability modeling for complex systems," *IEEE Transactions on Reliability*, vol. 72, no. 2, pp. 456–468, 2023.

[19] D. Kim and S. Lee, "Edge AI for real-time surveillance: Reliability and performance analysis," *IEEE Access*, vol. 11, pp. 22345–22360, 2023.

[20] M. Hassan and S. Ali, "Integrated risk management in smart security systems using hybrid models," *Safety Science*, vol. 147, 105621, 2022.

[21] T. Nguyen and B. Tran, "Reliability and availability analysis of cloud-based AI services," *Journal of Cloud Computing*, vol. 10, no. 1, 45, 2021.

[22] M. Rahman, S. Islam, and M. Rahman, "AI-driven predictive maintenance for industrial IoT systems," *Computers in Industry*, vol. 137, 103594, 2022.

[23] J. Torres and L. Martinez, "Reliability engineering in autonomous robotic systems: Challenges and solutions," *Robotics and Autonomous Systems*, vol. 142, 103789, 2021.

[24] F. Rossi et al., "Reliability challenges in autonomous robotic systems," *Robotics and Autonomous Systems*, vol. 171, 104593, 2024.

[25] S. Kuutti et al., "A survey of deep learning applications to autonomous vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 2, pp. 712–733, 2021.

[26] E. Zio, "The future of reliability engineering in the era of artificial intelligence," *Reliability Engineering & System Safety*, vol. 215, 107849, 2021.